Texte A

Mémoire à remettre 4 avril 23h59 au plus tard

Résumé : On étudie un protocole de mise en commun de secrets utilisant des matrices à coefficients dans un corps fini. Nous construisons ensuite deux attaques contre ce protocole, dont nous étudions le comportement afin de se protéger contre de mauvais choix de paramètres.

Mots clefs : algèbre linéaire, valeurs propres, corps finis.

► *Il est rappelé que le jury n'exige pas une compréhension exhaustive du texte. Vous êtes laissé(e) libre d'organiser votre discussion comme vous l'entendez. Des suggestions de développement, largement indépendantes les unes des autres, vous sont proposées en fin de texte. Vous n'êtes pas tenu(e) de les suivre. Il vous est conseillé de mettre en lumière vos connaissances à partir du fil conducteur constitué par le texte. Le jury appréciera que la discussion soit accompagnée d'exemples traités sur ordinateur.*

1. Introduction

La sécurité de certains protocoles de transfert d'information numérique est basée sur l'existence de fonctions dites *à sens unique*, c'est-à-dire des fonctions pour lesquelles les images des éléments sont effectivement calculables et ceci en temps raisonnable mais dont les images réciproques ne le sont pas. Il est bien sûr nécessaire, notamment pour les communications en temps réel, que les calculs soient effectués rapidement, à savoir que les algorithmes utilisés soient optimaux et leur implémentation optimale. À l'inverse, la recherche des images réciproques doit être inaccessible à l'échelle humaine aussi bien en temps de calcul qu'au niveau de la capacité des machines utilisées.

Ce texte étudie un exemple de telles fonctions dans le cadre d'un protocole permettant à deux correspondants $\mathscr{A}$ et $\mathscr{B}$ de se mettre d'accord sur un secret commun de façon sécurisée. Voici une brève description du protocole :

— $\mathscr{A}$ et $\mathscr{B}$ choisissent judicieusement un groupe G et un élément μ de ce groupe ;
— $\mathscr{A}$ choisit sa contribution au secret : a (un entier positif ou nul), calcule $s_{\mathscr{A}} = \mu^a \in G$ et l'envoie à $\mathscr{B}$;
— $\mathscr{B}$ choisit sa contribution au secret : b (un entier positif ou nul), calcule $s_{\mathscr{B}} = \mu^b \in G$ et l'envoie à $\mathscr{A}$;
— $\mathscr{A}$ et $\mathscr{B}$ calculent respectivement $(s_{\mathscr{B}})^a$ et $(s_{\mathscr{A}})^b$ qui sont deux quantités égales et deviennent leur secret commun.

Une fois ce partage réalisé, $\mathscr{A}$ et $\mathscr{B}$ peuvent utiliser leur secret commun pour échanger des informations confidentielles dans le cadre d'un protocole de chiffrement à clé secrète.

Un espion $\mathscr{C}$ qui aurait écouté les échanges entre $\mathscr{A}$ et $\mathscr{B}$ dispose des données suivantes :

$$G, \mu, s_{\mathscr{A}}, s_{\mathscr{B}}$$

et tente de s'immiscer dans la conversation entre $\mathscr{A}$ et $\mathscr{B}$. Le texte étudie des moyens d'y parvenir.

Contexte Dans toute la suite de ce texte, le groupe considéré sera le groupe des matrices inversibles de taille n à coefficients dans le corps fini $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Autrement dit : $G = \mathrm{GL}_n(\mathbb{F}_p)$.

2. Des paramètres à proscrire

Notations Étant donnée une matrice carrée M, on notera Π_M son polynôme minimal. Étant donnés deux polynômes P, Q à coefficients dans un corps, on note $\mathrm{Reste}(P,Q)$ le reste de P par la division euclidienne par Q.

Le problème à résoudre pour l'attaquant $\mathscr{C}$ est le suivant : *étant données trois matrices A, B et M de $\mathrm{GL}_n(\mathbb{F}_p)$, où $A = M^a$ et $B = M^b$ (mais ni a ni b ne sont connus), trouver $M^{ab} = A^b = B^a$.*

Une manière de résoudre ce problème consiste à retrouver $R_a := \mathrm{Reste}(X^a, \Pi_B)$, puis à calculer $R_a(B)$ ou à retrouver $R_b := \mathrm{Reste}(X^b, \Pi_A)$, puis à calculer $R_b(A)$. Nous allons nous focaliser sur la détermination de $\mathrm{Reste}(X^a, \Pi_B)$; la détermination de $\mathrm{Reste}(X^b, \Pi_A)$ s'obtiendra de façon analogue en remplaçant a par b et A par B.

Tout d'abord notons que l'on peut calculer le polynôme :

$$f := \mathrm{Reste}(X^a, \Pi_M). \tag{1}$$

Pour ce faire, on résout le système d'équations linéaires donné par :

$$f(M) = \sum_{i=0}^{\deg(f)} f_i M^i = A. \tag{2}$$

C'est un système de n^2 équations, d'inconnues $f_0, f_1, \ldots, f_{\deg(f)}$ et qui admet f comme unique solution. Les lemmes suivants nous fournissent deux situations dans lesquelles l'attaquant $\mathscr{C}$ pourra aisément retrouver le secret commun M^{ab}.

Lemme 1. *Si $a < \deg \Pi_M$, alors $f = X^a$.*

Lemme 2. *Si Π_B divise Π_M, alors $f(B) = M^{ab}$.*

On peut même aller plus loin en généralisant le Lemme 2 par le théorème suivant.

Théorème 1. *Soit P_B le plus petit commun multiple de Π_M et de Π_B. Il existe un unique polynôme g tel que $\deg(g) < \deg(P_B)$, $A = g(M)$ et $M^{ab} = g(B)$. De plus $g = f + \Pi_M h$ où $\deg(h) < \deg(P_B) - \deg(\Pi_M)$.*

Démonstration. Le polynôme g n'est rien d'autre que $\mathrm{Reste}(X^a, P_B)$. □

On ne dispose pas de méthode pour calculer le polynôme h du Théorème 1. Toutefois, si l'on évalue $(f+\Pi_M h)(B)$ pour tous les $p^{\deg(P_B)-\deg(\Pi_M)}$ choix possibles de h, on sait que l'un d'entre eux est le secret commun. $\mathscr{A}$ et $\mathscr{B}$ ont donc intérêt à ce que $\deg(P_B)-\deg(\Pi_M)$ soit le plus grand possible.

Conclusion Les correspondants $\mathscr{A}$ et $\mathscr{B}$ doivent choisir leurs contributions respectives au secret a et b de manière à ce que $a,b > \deg\Pi_M$ et Π_A,Π_B premiers à Π_M.

3. Calcul d'une contribution au secret commun

Dans le cadre précis de l'étude, le problème du calcul d'une contribution au secret commun de $\mathscr{A}$ et $\mathscr{B}$ peut s'énoncer comme suit : étant données deux matrices A et M de $\mathrm{GL}_n(\mathbb{F}_p)$ telles qu'il existe un entier a tel que $M^a = A$, trouver a.

Nous allons dans ce qui suit étudier un algorithme de réduction qui ramène le calcul dans le cadre matriciel à un certain nombre de calculs dans le cadre des corps finis, c'est-à-dire, étant donnés deux éléments σ et μ d'un corps fini $\mathbb{F}_{p^\ell}$ tels qu'il existe un entier α tel que $\sigma = \mu^\alpha$, trouver α. Nous ne chercherons pas à étudier la construction effective de solutions pour ce problème, mais nous le considérerons comme un calcul de référence dans $\mathbb{F}_{p^\ell}$ appelé *logarithme*.

Nous allons étudier l'ordre d'un élément dans $\mathrm{GL}_n(\mathbb{F}_p)$. Commençons un lemme :

Lemme 3. *Soit $\lambda \in \mathbb{F}_{p^\ell}^*$. L'ordre de X dans le groupe multiplicatif $(\mathbb{F}_{p^\ell}[X]/(X-\lambda)^t)^*$ est $p^\delta \mathrm{ord}(\lambda)$, où $\mathrm{ord}(\lambda)$ désigne l'ordre de λ dans $\mathbb{F}_{p^\ell}^*$ et δ est l'unique entier tel que $p^{\delta-1} < t \leqslant p^\delta$.*

Démonstration. L'assertion équivaut à déterminer l'ordre de $X+\lambda$ modulo X^t. Mais dans $\mathbb{F}_{p^\ell}$, pour j,k entiers, on a

$$(X+\lambda)^{jp^k} = \lambda^{jp^k} + j\lambda^{(j-1)p^k} X^{p^k}(1+S(X)), \tag{3}$$

avec $S \in \mathbb{F}_{p^\ell}[X]$, $S(0)=0$. Une étude des conséquences de cette identité conduit au résultat, en remarquant que l'ordre de λ est premier avec p. □

Nous en déduisons une forme explicite de l'ordre d'une matrice M :

Proposition 1. *Soit M une matrice de $\mathrm{GL}_n(\mathbb{F}_p)$, et Π_M son polynôme minimal. Notons $\Pi_M = f_1^{t_1}\dots f_s^{t_s}$ la décomposition en facteurs irréductibles de Π_M sur $\mathbb{F}_p$. Pour tout $i \in \{1,\dots,s\}$, on pose $m_i = \deg f_i$ et on se donne λ_i une racine de f_i dans $\mathbb{F}_{p^{m_i}}$.*

Soit t le maximum des t_i. Alors, l'ordre de M vérifie

$$\mathrm{ord}(M) = p^\tau \mathrm{ppcm}(\mathrm{ord}(\lambda_1),\mathrm{ord}(\lambda_2),\dots,\mathrm{ord}(\lambda_s)) \tag{4}$$

où τ est caractérisé par $p^{\tau-1} < t \leqslant p^\tau$.

Démonstration. Pour que $M^k = I_n$, il faut et il suffit que $\Pi_M | X^k-1$, ou encore que $X^k = 1 \bmod f_i^{t_i}$ pour tout i. Mais si $(X-\lambda_i)^{t_i} | (X^k-1)$, on a $(X-\lambda_i^{p^j})^{t_i} | (X^k-1)$ pour tout j, et donc $f_i^{t_i}$ divise X^k-1. □

La valeur de a modulo ord(M) peut alors être déterminée comme suit.

D'abord, pour chaque valeur propre λ, on note v un vecteur propre associé. Si N est une matrice inversible dont la première colonne est v alors la première colonne de $N^{-1}MN$ est $(\lambda, 0, \ldots, 0)$. Le calcul de $N^{-1}AN$ donne la valeur de λ^a. Le calcul de a modulo ord(λ) se ramène donc à un calcul de *logarithme* dans une extension de $\mathbb{F}_p$.

Il reste à obtenir la valeur de a modulo p^τ. On choisit un facteur de Π_M de multiplicité maximale t, et λ une valeur propre associée. On détermine un vecteur v solution de $(M-\lambda I)^t y = 0$, $(M-\lambda I)^{t-1} y \neq 0$. Si N est une matrice inversible dont les t premières colonnes sont les vecteurs $v_1, \ldots, v_t$ définis par

$$v_t = v \quad \text{et} \quad v_i = (M-\lambda I)v_{i+1} \quad i = t-1, \ldots, 2, 1, \tag{5}$$

alors, à l'image de ce qui précède, la matrice $N^{-1}MN$ est de la forme

$$N^{-1}MN = \begin{pmatrix} J & ? \\ 0 & ? \end{pmatrix}, \qquad \text{avec} \qquad J = \begin{pmatrix} \lambda & 1 & & (0) \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ (0) & & & \lambda \end{pmatrix}. \tag{6}$$

La matrice $N^{-1}AN$ est maintenant de la forme

$$\begin{pmatrix} J^a & ? \\ 0 & ? \end{pmatrix}. \tag{7}$$

De la connaissance de J^a, on déduit facilement $a \mod p$, par exemple en regardant le coefficient $(1,2)$ de cette matrice.

Une fois connu $u = a \mod p$, on sait que $a \bmod \text{ord}(M) = u + pv$ et donc

$$AM^{-u} = (M^p)^v. \tag{8}$$

Posant $A' = AM^{-u}$ et $M' = M^p$, il suffit de réutiliser la méthode qui précède pour obtenir, de proche en proche, la valeur de $a \bmod p^\tau$.

Le fait de travailler avec des matrices ne change donc pas significativement la difficulté du problème posé, par rapport à utiliser un groupe $G = \mathbb{F}^*_{p^\ell}$.

4. Sous-ensemble de matrices particulières

Nous allons maintenant nous intéresser au problème du paragraphe précédent dans le cadre particulier des matrices inversibles à coefficients dans $\mathbb{F}_p$ de la forme :

$$M(a_0, \ldots, a_{n-1}) = \begin{pmatrix} a_0 & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \ldots & a_{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ a_1 & a_2 & a_3 & \ldots & a_0 \end{pmatrix}. \tag{9}$$

Autrement dit les matrices $n \times n$ dont les lignes, à partir de la deuxième, sont des permutations circulaires de la première. Ces matrices sont donc définies par leur première ligne.

L'ensemble des matrices de taille n de ce type, que nous noterons $C_n(\mathbb{F}_p)$, muni de l'addition et de la mutiplication des matrices forme un anneau commutatif isomorphe à l'anneau quotient $\mathbb{F}_p[X]/(X^n-1)$. En effet, toute matrice de ce type peut s'écrire comme polynôme en la matrice $M(0,1,0,\dots,0)$.

Rappelons que l'on cherche ici, étant données deux matrices A et M de $C_n(\mathbb{F}_p)$, à trouver un a tel que $M^a = A$.

Nous supposons maintenant que p ne divise pas n. On peut alors mener l'étude de la sécurité en s'appuyant sur l'isomorphisme explicite

$$C_n(\mathbb{F}_p) \cong \mathbb{F}_p[X]/(X^n-1) \cong \prod_{i=1}^{r} \mathbb{F}_p[X]/(P_i(X)), \tag{10}$$

où $X^n - 1 = \prod_{i=1}^{r} P_i(X)$ est la factorisation de X^n-1 dans $\mathbb{F}_p$, avec par exemple $P_1 = X-1$.

Théorème 2. *Soit ℓ un nombre premier, et notons s l'ordre de p modulo ℓ. Alors le polynôme $(X^\ell-1)/(X-1)$ se décompose en un produit de $(\ell-1)/s$ facteurs irréductibles de degré s dans $\mathbb{F}_p$.*

Démonstration. Soit ω une racine primitive ℓ-ème de l'unité dans une clôture algébrique de $\mathbb{F}_p$. Alors les polynômes

$$R_i(X) = (X-\omega^i)(X-\omega^{pi})\dots(X-\omega^{p^{s-1}i}) \tag{11}$$

sont à coefficients dans $\mathbb{F}_p$ pour tout i. En choisissant bien les valeurs de i, on trouve $(\ell-1)/s$ facteurs de degré s deux-à-deux distincts.

Supposons maintenant que $R_i(X)$ admet un facteur de degré $0 < s' < s$. Dans ce cas, on a $\omega^i \in \mathbb{F}_{p^{s'}}$, soit $\omega^{ip^{s'}} = \omega^i$, ce qui est impossible si $i \neq 0$. □

En particulier, le choix optimal de paramètre pour le protocole de cette partie semble être le cas où n est un nombre premier, et où p est d'ordre $n-1$ modulo n – reste encore à choisir M d'ordre maximal dans $C_n(\mathbb{F}_p)$.

Suggestions pour le développement

► *Soulignons qu'il s'agit d'un menu à la carte et que vous pouvez choisir d'étudier certains points, pas tous, pas nécessairement dans l'ordre, et de façon plus ou moins fouillée. Vous pouvez aussi vous poser d'autres questions que celles indiquées plus bas. Il est très vivement souhaité que vos investigations comportent une partie traitée sur ordinateur et, si possible, des représentations graphiques de vos résultats.*

— Tout au long du texte, plusieurs faits ou résultats sont énoncés sans démonstration, ou avec des démonstrations incomplètes. On pourra en justifier certains.
— Préciser les allusions faites à la complexité des opérations dans les divers structures présentes dans le texte.
— Discuter l'efficacité de la méthode du paragraphe 3 ; combien de calculs de logarithme dans une extension $\mathbb{F}_p$ faut-il faire ? Combien d'autres opérations ?

— Dans la section 4, quel est alors l'avantage à considérer des matrices à coefficients dans $\mathbb{F}_p$ plutôt que de considérer une extension de $\mathbb{F}_p$?

— À l'aide des méthodes de la Section 2 peut-on calculer le secret commun lorsque $p = 29$ et

$$M = \begin{pmatrix} 7 & 4 & 12 \\ 13 & 19 & 10 \\ 15 & 9 & 26 \end{pmatrix} \quad A = \begin{pmatrix} 14 & 7 & 4 \\ 9 & 3 & 17 \\ 12 & 4 & 6 \end{pmatrix} \quad B = \begin{pmatrix} 8 & 6 & 4 \\ 15 & 15 & 18 \\ 21 & 26 & 23 \end{pmatrix} ?$$

— De même, peut-on trouver un ensemble de matrices le plus petit possible qui contienne le secret commun lorsque $p = 29$ et

$$M = \begin{pmatrix} 5 & 1 & 2 \\ 26 & 23 & 3 \\ 16 & 21 & 20 \end{pmatrix} \quad A = \begin{pmatrix} 6 & 24 & 19 \\ 15 & 3 & 14 \\ 7 & 11 & 18 \end{pmatrix} \quad B = \begin{pmatrix} 7 & 19 & 9 \\ 1 & 1 & 28 \\ 14 & 22 & 2 \end{pmatrix}.$$

— Quel est l'ordre de la matrice de $\mathrm{GL}_n(\mathbb{F}_{29})$ suivante :

$$\begin{pmatrix} 8 & 26 & 0 \\ 2 & 11 & 11 \\ 6 & 8 & 20 \end{pmatrix} ?$$

— Dans la dernière partie, quelle information peut-on obtenir si $\sum_{i=0}^{n-1} a_i \neq 1$?

— Même question que la précédente si le déterminant de $M(a_0, \ldots, a_{n-1})$ est distinct de 1.

— Discuter le coût du calcul des valeurs propres des matrices $M(a_0, \ldots, a_{n-1})$.